1. INTRODUCTION TO MODULAR ARITHMETIC

If someone asks you what day it is 145 days from now, what would you answer? Would you count 145 days, or find a quicker way? Maybe, you would note that there are 7 days in a week, and, therefore, in seven days it would be the same day as today. Then you would only have to find out how many groups of 7 fit into 145. This could be easily done by dividing 7 into 145. The answer, of course, would be 20, with 5 left over, or \( 145 = 7(20) + 5 \). Then, it would only be necessary to count 5 days from today, and you would see that it would Saturday.

You may think this knowledge would only be useful to show off to friends, but you would be mistaken. Programmers use this information to write calendar programs, and time programs, as well as others.

The mathematics that is involved in this problem is called modular arithmetic. Instead of looking at a number as a value in and of itself, it is though of as a member of a remainder class relative to a number.

For Example, if we wanted to compute \( 12 \mod (5) \) we would see that \( 12 = 5(2) + 2 \), and therefore, 5 goes into 12 twice with remainder 2. Hence, \( 12 \mod (5) = 2 \).

See if you can compute the following:

(a) \( 17 \mod (3) \)
(b) \( 39 \mod (4) \)
(c) \( 137 \mod (6) \)
(d) \( 234 \mod (10) \)
(e) $365 \mod (7)$

(f) $73 \mod (52)$

(g) $256 \mod (12)$

Why were the last three problems significant? Could you think of word problems that might be associated to those computations?

Problem 1. How many years would it take for August 6 to be a Monday?

2. Modular Congruence

What does it mean that $7 \equiv 2 \mod (5)$?

First of all, it means that the difference of 7 and 2 is a multiple of 5, i.e.,

$$7 - 2 = 5k$$

for some integer, $k$.

Is 7 actually equal to 2. What does equivalent mean?

An equivalence relation is a relation that is symmetric, reflexive and transitive. Symmetry means, since

$$7 \equiv 2 \mod (5)$$
then

\[ 2 \equiv 7 \mod (5). \]

Reflexive means that \( 2 \equiv 2 \mod (5) \) and transitive means that if \( 2 \equiv 7 \mod (5) \) and \( 17 \equiv 2 \mod (5) \) then \( 17 \equiv 7 \mod (5) \). The modulo 5 congruence class of 2 is

\[ \{ \cdots -23, -18, -13, -8, -3, 2, 7, 12, 17, 22, 27, \ldots \} \]

We call \( 2 \) the residue of this class modulo 5 and we call the congruence class, the residue class.

**Lemma 1.** Let \( a, b, n \in \mathbb{Z} \) be integers.
The relation \( a \equiv b \) if and only if \( a \equiv b \mod (n) \) is an equivalence relation.

**Proof 1.** We will prove that modulo is an equivalence relation by proving that it is symmetric, reflexive and transitive.

**symmetry**

By definition, \( a \equiv b \mod (n) \) implies that \( a - b = nk \) for some integer \( k \). Therefore, \( b - a = -nk = n(-k) \) where \(-k \in \mathbb{Z}\). Therefore, \( b \equiv a \mod (n) \).

**reflexive** Since \( a - a = n(0) \) and 0 is an integer, then by definition, \( a \equiv a \mod (n) \).

**transitive** Suppose \( a \equiv b \mod (n) \) and \( b \equiv c \mod (n) \), then by definition,

\[ a - b = nk_1 \quad \text{and} \quad b - c = nk_2 \]

Therefore, by adding both equations together, we get

\[ a - b + b - c = nk_1 + nk_2 \]

Simplification and factoring yields the desired result,

\[ a - c = n(k_1 + k_2) \]

where \( k_1 + k_2 \) is an integer, and therefore \( a \equiv c \mod (n) \).

3. **Adding and Subtracting**

Suppose you want to add two numbers modulo \( m \). Would you be able to just add their residues? We’d like to believe that to be the case. Let’s look at an Example.

**Example 1.** Suppose you want to add 7 and 23 modulo 6.

\[ 7 + 23 = 30 \mod (6) = 0 \]

and

\[ 7 \mod (6) = 1 \quad \text{and} \quad 23 \mod (6) = 5, \quad \text{so} \quad 1 + 5 = 0 \mod (6). \]

Well, that was nice. I hope it happens like that all the time. Let’s see.

**Lemma 2.** Let \( r_1 = a \mod (n) \) and \( r_2 = b \mod (n) \),
then \( r_1 + r_2 \mod (n) = a + b \mod (n) \).
Proof 2. If \( r_1 = a \mod (n) \), then \( r_1 - a = nk_1 \).

Also, \( r_2 = b \mod (n) \) then \( r_2 - b = nk_2 \).

So if we add both equations together, we get

\[
r_1 - a + r_2 - b = nk_1 + nk_2
\]

\[
(r_1 + r_2) - (a + b) = n(k_1 + k_2)
\]

where \( k \) is an integer. Therefore, by definition, \((r_1+r_2) = (a+b) \mod (n)\)

From this we can see that \(-r = n - r \mod (n)\).

4. Exercises

Exercise 1. Add the following and simplify:

(a) \( 73 + 89 \mod (10) \)

(b) \( 93 + 47 \mod (9) \)

(c) \( 403 - 397 \mod (8) \)

(d) \( 1214 + 1591 \mod (7) \)

(e) \( 134 + 453 - 217 \mod (12) \)

(f) \( 2372 + 971 - 1549 \mod (11) \)

Exercise 2. Find the additive inverse of each number in the respective modulo class.

(a) \( 5 \mod (9) \)

(b) \( 7 \mod (12) \)

(c) \( 4 \mod (8) \)

Exercise 3. Find the value(s) for \( x \) that make the equation true.

(a) \( x + 6 = 2 \mod (7) \)

(b) \( x + 117 = 73 \mod (125) \)
5. Multiplication and Division

Lemma 3. Let \( r_1 = a \mod (n) \) and \( r_2 = b \mod (n) \), then \( r_1 r_2 \mod (n) = ab \mod (n) \)

Proof 3. If \( r_1 = a \mod (n) \), then \( a = nk_1 + r_1 \). This is equivalent to

\[
ab = (nk_1 + r_1)(nk_2 + r_2)
\]

\[
ab = n(nk_1k_2 + r_1nk_2 + r_2nk_1 + r_1r_2)
\]

where \( nk_1k_2 + r_1k_2 + r_2k_1 \) is an integer.

Therefore, by definition, \( (r_1r_2) = (ab) \mod (n) \)

Corollary 1. If \( a = b \mod (n) \) then \( a^n = b^n \mod (n) \).

The corollary above follows from the fact that multiplication respects modulo classes.

6. Exercises

Exercise 4. Compute each of the following:

(a) \( 23 \cdot 17 + 7 \mod (4) \)

(b) \( 121 \cdot 122 \cdot 123 \mod (5) \)

(c) \( 11 \cdot 23 - 5 \cdot 28 \mod (10) \)

(d) \( 514 \cdot 891 \mod (11) \)

(e) \( 4^4 \mod (5) \)

(f) \( 2^4 \mod (5) \)

(g) \( 3^4 \mod (5) \)

(h) \( 2^6 \mod (7) \)

(i) \( 3^6 \mod (7) \)

Do you see a pattern above?

What do you think is true in general?
Try the following:

(a) \(2^5 \mod (6)\)

(b) \(2^7 \mod (8)\)

(c) \(2^{10} \mod (11)\)

Do you see a pattern? Would you like to change your conjecture?

The proof that if \(p\) is prime, then for any nonzero number \(n\), \(n^{p-1} = 1 \mod (p)\) requires group theory. However, we may get a glimpse of this through the following exercises.

7. The multiplicative group modulo \(n\)

<table>
<thead>
<tr>
<th>(5^p)</th>
<th>Simplify</th>
<th>mod(?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(5^1)</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>(5^2)</td>
<td>25</td>
<td>4</td>
</tr>
<tr>
<td>(5^3)</td>
<td>4 \cdot 5</td>
<td>6</td>
</tr>
<tr>
<td>(5^4)</td>
<td>6 \cdot 5</td>
<td>2</td>
</tr>
<tr>
<td>(5^5)</td>
<td>2 \cdot 5</td>
<td>3</td>
</tr>
<tr>
<td>(5^6)</td>
<td>3 \cdot 5</td>
<td>1</td>
</tr>
<tr>
<td>(5^7)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5^8)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5^9)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5^{10})</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5^{11})</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5^{12})</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5^{13})</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5^{14})</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What did you notice?

Was there a pattern? How long was it?

Let’s try another one.

<table>
<thead>
<tr>
<th>(5^p)</th>
<th>Simplify</th>
<th>mod(8)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(5^1)</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>(5^2)</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>(5^3)</td>
<td>1 \cdot 5</td>
<td>5</td>
</tr>
<tr>
<td>(5^4)</td>
<td>5 \cdot 5</td>
<td>1</td>
</tr>
</tbody>
</table>

What did you notice now?

Was there a pattern? How long was it?
Try the same thing on a separate sheet of paper with the following numbers:

(a) Powers of 3 modulo 8
(b) Powers of 4 modulo 8
(c) Powers of 6 modulo 8
(d) Powers of 7 modulo 8
(e) Powers of 4 modulo 7
(f) Powers of 6 modulo 7
(g) Powers of 2 modulo 7

Now we can use these patterns to find higher powers. Have you found a higher power? Do you feel the higher power? Just kidding. Let’s get back to math.

8. Exercises

Exercise 5. Find the remainder of the following modulo 5:
(a) $2^8$
(b) $3^{19}$
(c) $4^{55}$
(e) $19^{77}$
(f) $14^{92} \cdot 17^{76}$
Exercise 6.  (A) Find all possible residues of a perfect square modulo 4.

(B) Use the information you learned from part (A) to show that there are no solutions to the equation $a^2 + b^2 = 10511$.

Exercise 7. Find the units digit of $9^{87}$.

9. CHALLENGE

Problem 2 (Mathematical Circles). Find

$$10^{10} + 10^{100} + 10^{1000} + \cdots + 10^{10000000000}$$

Problem 3 (AMC). What is the size of the largest subset $S$ of \{1, 2, 3, \ldots, 50\} such that no pair of distinct elements of $S$ has a sum divisibly by 7.

Problem 4. The Fibonacci sequence is defined by $F_1 = F_2 = 1$ and $F_{n+2} = F_{n+1} + F_n$. Find $F_{2006} \mod (5)$.
10. Multiplicative Inverses modulo n

Recall the Euclidean Algorithm for finding the $gcd(a, b)$ of two integers $a$ and $b$.

$$a = bq_1 + r_1$$
$$b = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$
$$r_2 = r_3q_4 + r_4$$

... 

$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1}$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$
$$r_{n-1} = r_nq_{n+1}$$

Recall that one stops when the last remainder is zero. The last nonzero remainder $r_n$ is the $gcd(a, b)$ We can substitute each equation into the previous and rearrange it so that we get a linear combination of $a$ and $b$ equal to $r_n$. So that we don’t confuse the $gcd(a, b)$ for any other remainder, we will henceforth denote $r_n = d$.

$$d = r_{n-2} - r_{n-1}q_{n-1}$$
$$d = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-2})q_{n-1}$$
$$d = (r_{n-4} - r_{n-3}q_{n-3}) - (rn - 3 - (r_{n-4} - r_{n-3}q_{n-3})q_{n-2})q_{n-1}$$

As you can see, we can substitute backwards until we reach the sum of multiples of $a$ and $b$ only. Therefore, if $gcd(a, b) = d$, then

$$d = am + bk$$

implies that there exists solutions to the equations $ax \equiv d \mod (b)$ and $bx \equiv d \mod (a)$ by reducing the equations modulo $b$ or $a$, respectively.

This is why only numbers relative prime to $b$ will have multiplicative inverses.

If two numbers are relatively prime, then $gcd(a, b) = 1$ and therefore, $1 = am + bk$. If we mod out by $b$, then we get

$$1 = am \mod (b)$$

Or in other words, there is an integer, $m$, such that $am = 1 \mod (b)$. Therefore, $m$ is the multiplicative inverse of $a$. 

11. Exercises

Exercise 8. Find the multiplicative inverse, if any, of each elements below.

(a) $4 \mod (10)$

(b) $5 \mod (11)$

(c) $7 \mod (12)$

(d) $3 \mod (9)$

(e) $7 \mod (10)$

Exercise 9. Use your new knowledge of multiplicative inverses to find the solution to the equations below, if any.

(a) $2x + 3 = 6 \mod (7)$

(b) $3x - 7 = 0 \mod (8)$

(c) $3x^2 - 1 = 0 \mod (5)$

12. Checking for divisibility by $n$

In this section we will learn all the tricks that allow us to see if a number is divisibly by another without putting in too much work.

Lemma 4 (Divisibility by 3). A number is divisible by 3 if its digits are divisibly by 3.

Proof 4. Let $n \in \mathbb{Z}$ be an integer.
Suppose its base 10 representation is

$$n = a_010^0 + a_110^1 + a_210^2 + a_310^3 + \cdots a_n10^n$$

$n$ is divisible by 3 if and only if $n = 0 \mod (3)$.
So let’s mod out the entire equation above by 3.

$$n \mod (3) = a_0 + a_1 + a_2 + \cdots + a_n$$

Where did all the powers of 10 go?
Well, if you remember $10 = 1 \mod (3)$, and therefore, all powers of 10 are also $1 \mod (3)$.
Hence, $a n = 0 \mod (3)$ if and only if $a_1 + a_2 + \cdots + a_n = 0 \mod (3)$.
The same proof will give us \( n = 0 \mod (9) \) if its digits are divisible by 9 because \( 10 = 1 \mod (9) \).

**Corollary 2.** Every number is in the same residue class mod 3 as the sum of its digits.

The above corollary follows from the proof, but is a more general statement.

**Lemma 5.** A number \( n \) is divisible by \( 2^m \) if its last \( m \) digits are divisible by \( 2^m \).

**Proof 5.** Let \( n = \sum_{n=0}^{k} a_n 10^n \). Then the last \( m \) digits can be achieved by \( n \mod (10^m) \).

Suppose \( n = r \mod (10^m) \), then \( n = 10^m q + r \) where \( q \) is an integer.

Since 2 is a factor of 10 then, \( 10^m = 2^m k \) for some integer \( k \).

By substitution, \( n = (2^m k) q + r \). So as you can see, \( n = r \mod (2^m) \).

Therefore, if \( r = 0 \mod (2^m) \), then the last \( m \) digits are divisible by \( 2^m \).

Since \( n = r \mod (2^m) \), then \( n = 0 \mod (2^m) \).

**Corollary 3.** A number \( n \) is divisible by \( 5^m \) if its last \( m \) digits are divisible by \( 5^m \).

A similar proof will result in the corollary above if you replace \( 2^k \) with \( 5^k \).

**Lemma 6.** A number \( n \) is divisible by 11 if the alternating sum of its digits is divisible by 11.

**Proof 6.** Suppose \( n \) is a number whose base 10 representation is given by

\[
n = \sum_{i=0}^{k} a_i (10^i)\]

Now if \( n \) is divisible by 11, then \( n = 0 \mod (11) \). Which means that

\[
\sum_{i=0}^{k} a_i (10^i) \mod (11) = \sum_{i=0}^{k} a_i (10 \mod (11))^i
\]

Since \( 10 \mod (11) = -1 \), then the sum above becomes

\[
n = \sum_{i=0}^{k} a_i (-1)^i \mod (11)
\]

Therefore, \( n = 0 \mod (11) \) if and only if \( \sum_{i=0}^{k} a_i (-1)^i = 0 \mod (11) \). This is the alternating sum of the digits of \( n \).
Lemma 7. A number $n = \sum_{i=0}^{k} a_i(10^i)$ is divisible by 7, if $[\sum_{i=1}^{k} a_i(10^i)] - 2a_0$ is divisible by 7.

Proof 7. Let’s assume that $n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10^2 a_3 + 10 a_2 + 10 a_1 + a_0$. Suppose that we apply the algorithm to $n$ and we get a multiple of 7.

$$10^{k-1} a^k + 10^{k-2} a_{k-1} + \cdots + 10^2 a_3 + 10 a_2 + a_1 - 2a_0 = 0 \mod (7)$$

$$3^{k-1} a^k + 3^{k-2} a_{k-1} + \cdots + 2a_3 + 3a_2 + a_1 - 2a_0 = 0 \mod (7)$$

$$3^{k-1} a^k + 3^{k-2} a_{k-1} + \cdots + 2a_3 + 3a_2 + a_1 + 5a_0 = 0 \mod (7)$$

Multiplying the equation by the multiplicative inverse of 5 mod (7)

$$3^k a^k + 3^{k-1} a_{k-1} + \cdots + 6a_3 + 2a_2 + 3a_1 + a_0 = 0 \mod (7)$$

$$10^k a^k + 10^{k-1} a_{k-1} + \cdots + 10^3 a_3 + 10^2 a_2 + 10 a_1 + a_0 = 0 \mod (7)$$

So if we take the units digit of $n$, and subtract it from the remaining digits, and the result is 0 mod (7) then $n$ is.

A similar algorithm can be used for any prime number relatively prime to 10. Why?
The only difference is that you find another multiple of the units digit to subtract from the rest of the digits.

13. Exercises

State whether the following numbers are divisible by 3, 9, or 11.

(a) 178123

(b) 5472

(c) 332175

(d) 172271

(e) 1721271
State whether the following are multiples of 8.
(a) 1444
(b) 83412
(c) 971352
(d) 22222220

State whether the following are multiples of 7.
(a) 672
(b) 902
(c) 3976
(d) 273

Find a similar algorithm to check for divisibility for 13

14. Challenge Problems

Problem 5. How many four digit palindromes are multiples of 9?

Problem 6. Find a six-digit number whose first three digits are 523 such that the integer is divisibly by each 7, 8, 9.
Problem 7. What is the smallest 5-digit palindrome that is a multiple of 99?

Problem 8. Prove that a power of 2 cannot end in four equal digits?

Problem 9. The integer $n$ is the smallest positive multiple of 15 such that every digit of $n$ is either 0 or 8. Compute $\frac{n}{15}$. (AIME)